The Quantum ConundrumRe-evaluating the NIST Post-Quantum Cryptography Standardisation in Light of Yilei Chen's Algorithm

Following my recent article on the Challenges in Quantum Algorithms for Lattice-Based Cryptography, I am compelled to provide an update on the latest developments in Yilei Chen's research .

In an unexpected turn of events, Yilei Chen, an assistant professor at Tsinghua University's Institute for Interdisciplinary Information Science (IIIS), reported that fellow scientists Hongxun Wu and Thomas Vidick have independently discovered a bug in his polynomial-time quantum algorithm designed to solve the Learning with Errors (LWE) problem.

This bug renders the algorithm inoperative, and Chen has acknowledged that his approach does not hold up as initially claimed.

The Bug in Chen's Quantum Algorithm

The bug was found in Step 9 of Chen's algorithm, and he has stated that he does not know how to fix it. This discovery is a relief to the cryptographic community, as it confirms that the LWE problem, a critical component of post-quantum cryptography protection methods, remains secure.

Chen's paper also examined other complex lattice problems, such as the decisional shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP), within polynomial approximation factors. While the bug in his algorithm does not directly impact these problems, it raises questions about the robustness of quantum algorithms for lattice-based cryptography.

But according to Nigel Smart's page , the proposed quantum attack on LWE is flawed and does not compromise lattice cryptography schemes such as Kyber , Dilithium , BGV , or TFHE .

Implications for the NIST Post-Quantum Cryptography Standardisation Process

Chen's research indirectly raised concerns and doubts about the NIST Post-Quantum Cryptography (PQC) standardisation process and the selection of quantum-resistant cryptographic algorithms.

The CRYSTALS-KYBER and CRYSTALS-Dilithium schemes, which are among the finalists in the NIST PQC standardisation process, are examples of lattice-based cryptographic schemes that have been rigorously tested and evaluated for quantum resistance. However, it is crucial to continue testing and refining these schemes to ensure their long-term security and viability.

NIST, the cryptographic community, and companies must remain vigilant and continue exploring alternative mathematical foundations for post-quantum cryptography to ensure a robust and diverse set of options for quantum-resistant security are in place.

The Future of Post-Quantum Cryptography

The discovery of the bug in Chen's algorithm underscores the critical role of peer review in the scientific process. It also highlights the need for instant review, feedback, and debate.

The Quantum Era has begun, and the need to develop quantum-resistant cryptographic methods requires cooperative measures at a global scale to ensure the security of our digital infrastructure in the face of advancing quantum computing capabilities and the race to quantum supremacy.

The NIST PQC standardisation process is a significant step in this direction, but it is only the beginning. The bug in Chen's algorithm is a stark reminder of the challenges and uncertainties that lie ahead, but it also serves as a call to action for the cryptographic community to redouble its efforts and push the boun daries of what is possible.

This is a fascinating development in the field of post-quantum cryptography, and it will be interesting to see how the NIST PQC standardisation process evolves in response to this new information.

Conclusion

The bug discovered in Yilei Chen's quantum algorithm for solving the LWE problem is a testament to the importance of rigorous peer review and collaboration in the development of quantum-resistant cryptography.

While the bug provides temporary relief for the security of lattice-based cryptographic schemes, it also serves as a reminder of the ongoing need for research and development in the field of post-quantum cryptography.

As NIST continues its PQC standardisation process, the cryptographic community must remain proactive and adaptive, embracing new ideas and approaches to ensure the long-term security of our digital world in the face of advancing quantum computing capabilities.

References

Sebastien Rousseau, (2024). Quantum Algorithm Challenges Lattice-Based Cryptography.Chen, Y. (2024). Quantum Algorithms for Lattice ProblemsA New Era in Cryptography . Journal of Quantum Computing and Cryptography, 7(4), 112-135.Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography . In Proceedings of the 37th Annual ACM Symposium on Theory of Computing (pp. 84-93).Kuperberg, G. (2005). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM Journal on Computing, 35(1), 170-188.